PRIVACY LAWS AND THE EMPLOYER-EMPLOYEE RELATIONSHIP

A "LEGAL FOUNDATIONS" STUDY

Report 9 of 12

Report to the
President's Commission
on Critical Infrastructure Protection
1997

This report was submitted to the President's Commission on Critical Infrastructure Protection, and informed its deliberations and recommendations. This report represents the opinions and conclusions solely of its developers.

Contents

Page

Acknowledgments ..... **iii**

Preface ..... **iv**

Part One: Introduction **1**
Research Findings 1
Assumptions 2

Part Two: Background **4**
Considerations for Employees in Sensitive Positions 6
Relevant Law and Legislation 7

Part Three: Approaches for Addressing Privacy Issues **17**
General Recommendation By the Federal Government That States Individually Examine Potential Unintended Consequences of Related Legislation And Consider Benefits of Adopting Unified Approaches 17
Federal Government Points Out Benefits of States Voluntarily Adopting Minimal Consensual "Baseline" For Acquisition of Background Information, At Least for Owners and Operators of Critical Infrastructures 18
The Administration Can Name a Panel To Consider Best Approach to Achieving Legislative Balance Between Security Needs and Privacy Interests 19
Congress And The Administration Can Recommend Narrow Amendments To *Federal* Privacy Laws To Serve As Model for State Legislative Reform 19
The Administration Can Recommend Limited Congressional Preemption Of State Privacy Laws To Accommodate Data Collection Needs 20

Part Four: Conclusions **21**
Diversity of State and Federal Law 21
Insider Threats to the Critical Infrastructures 22
Employee Screening Procedures 22
Fair Information Practices 23
Advocating a “Consensual Baseline” Approach 23
Privacy – Security Study Group 24
Illustrative Amendments to Federal Legislation 25

Appendices
Appendix A: Proposed Amendment to EPPA A-1

Acknowledgments

The *Legal Foundations* series of reports of the President's Commission on Critical Infrastructure Protection (PCCIP) resulted from the concerted efforts and hard work of several individuals. The Commission gratefully acknowledges Commissioner Stevan D. Mitchell and Assistant General Counsel Elizabeth A. Banker for their leadership and important contributions in developing the *Legal Foundations* series of reports. Their research, writing and analytical contributions were essential to the success of the effort.

The Commission also acknowledges Lee M. Zeichner, Esq. of LegalNet Works Incorporated and his staff, for conceptualizing and maintaining the legal issues database and for providing tireless research support. Finally, the Commission acknowledges the contributions of Senior Consultant Paul Byron Pattak for his deft editing of this compilation.

Preface

Executive Order 13010 established the President's Commission on Critical Infrastructure Protection (PCCIP) and tasked it with assessing the vulnerabilities of, and threats to, eight named critical infrastructures and developing a national strategy for protecting those infrastructures from physical and cyber threats. The Executive Order also required that the PCCIP consider the legal and policy issues raised by efforts to protect the critical infrastructures and propose statutory and regulatory changes necessary to effect any subsequent PCCIP recommendations.

To respond to the legal challenges posed by efforts to protect critical infrastructures, the PCCIP undertook a variety of activities to formulate options and to facilitate eventual implementation of PCCIP recommendations by the Federal government and the private sector. The PCCIP recognized that the process of infrastructure assurance would require cultural and legal change over time. Thus, these activities were undertaken with the expectation that many would continue past the life of the PCCIP itself.

The *Legal Foundations* series of reports attempts to identify and describe many of the legal issues associated with the process of infrastructure assurance. The reports were used by the PCCIP to inform its deliberations. The series consists of 12 reports:

1. *Legal Foundations: Studies and Conclusions*
2. *The Federal Legal Landscape*
3. *The Regulatory Landscape*
4. *Legal Authorities Database*
5. *Infrastructure Protection Solutions Catalog*
6. *Major Federal Legislation*
7. *Adequacy of Criminal Law and Procedure (Cyber)*
8. *Adequacy of Criminal Law and Procedure (Physical)*
9. *Privacy and the Employer-Employee Relationship*
10. *Legal Impediments to Information Sharing*
11. *Federal Government Model Performance*
12. *Approaches to Cyber Intrusion Response*

and two special studies:

- *Information Sharing Models*
- *Private Intrusion Response*

Legal Foundations: Studies and Conclusions is the overall summary report. It describes the other reports, the methodologies used by the researchers to prepare them, and summarizes the possible approaches and conclusions that were presented to the PCCIP for its consideration. The series has been sequenced to allow interested readers to study in detail a specific area of interest. However, to fully appreciate the scope of the topics studied and their potential interaction, a review of the entire series is recommended.

Part One

Introduction

This paper examines what the Federal government should do, if anything, to insure that appropriate legal means exist by which governments and the private sector can collect, retain and disseminate data or information integral to achieving infrastructure assurance objectives while respecting fundamental privacy concerns of individuals and the interests of state legislatures in protecting citizens' privacy. The paper explores the possibility of making available to owners and operators, for use in filling certain sensitive positions within the critical infrastructures, some of the techniques and methods currently used by the Federal government to screen employees for employment in certain sensitive positions.

Research Findings

- "Insider" misconduct is the most immediate and, to some, the most predominant security concern of infrastructure owners and operators. Insiders pose a potential threat along physical and cyber dimensions.
- Insider harm can prove more devastating than outsider harm by virtue of the insider's superior knowledge and access.
- Employee screening and employee monitoring are two techniques by which employers can impose additional security in the workplace. Of the two, employee screening appears to be the least intrusive.
- In 1994, Congress attempted to strike the delicate balance between the employer's right to monitor and employees' privacy interests in a series of comprehensive legislative proposals. The failure of those efforts demonstrates the difficulty and sensitivity of the issue.
- Enhanced employee screening, resembling measures taken by the Federal government in issuing security clearances, may prevent or deter some forms of insider misconduct.

- Efforts to prevent insider harm through more stringent employee screening implicate employee privacy issues, necessitating that a balance be struck between privacy and security:

    - ♦ Employers may wish to take into account in employment decisions factors such as criminal history, employment history, credit history, or even the results of a polygraph examination.

    - ♦ Individuals have a strong interest in controlling collection and dissemination of such highly personal (and potentially unreliable) information.

- Information technology exacerbates this potential clash of interests by increasing the ease with which such information might be collected, stored and disseminated.

- State lawmaking bodies have been responsive to citizens' privacy concerns, particularly where electronically stored information is concerned, and have enacted measures designed to protect sensitive information from collection or disclosure.

- Though responsive, the states have not adopted uniform approaches to these information privacy issues. This has resulted in a rich and varied "patchwork" of laws governing, among other things, the employer-employee relationship.

- This patchwork of privacy protections applies predominantly to private sector employees. Federal, state and local government employees are often expressly exempt.

- Federal laws have been established in some instances within this environment to unify divergent approaches, or to protect or restore vital national security concerns.

Assumptions

- Some state and Federal employee "privacy" laws, though enacted with best intentions, may unduly restrict the collection or dissemination of information that might otherwise be used by an owner or operator of the critical infrastructures to enhance infrastructure assurance.

- The elimination of some undue restrictions on collecting and sharing job-related information (at least for the owners and operators of critical infrastructures seeking to fill key positions) would permit and encourage owners and operators to avail themselves of employee screening procedures akin to those used by the government in issuing security clearances.

- Allowing owners and operators to more carefully pre-screen employees or prospective employees for certain sensitive positions within the critical infrastructures will enhance infrastructure assurance.

Part Two

Background

One the most pressing and complex problems facing our nation's critical infrastructures is the threat posed by their own employees. In a recent survey, 87 percent of respondents cited "disgruntled employees" as the likely source of computer attacks on their company.[1] Despite the alarming percentage of computer-related incidents, and the persistence of traditional criminal activity by insiders ($120 billion in employee theft each year),[2] few recommendations have been made in the area to date. The reluctance to address this problem may be traced to concerns among legislators, at the Federal and state levels, over infringing on the legitimate privacy interests of upstanding citizens. "The employer's interest in maintaining an honest workplace is not always consistent with the employee's interest in privacy."[3]

In fact, the trend in state legislation has been toward increasing the protections of employees and prospective employees from employer incursions into their personal privacy. These state statutes may forbid anything from inquiring about personal relationships to investigating criminal histories. While many of these statutes are well-crafted and serve the interests of employees and employers alike, others may be over-inclusive and ultimately inhibit infrastructure owners and operators from taking necessary security precautions.[4]

Not only is addressing the "insider threat" difficult because of the privacy interests at stake, but there are also difficult federalism concerns that must be considered. The Federal government has jurisdiction over the critical infrastructures through the interstate commerce power, and has in the past regulated some of the infrastructures quite heavily. However, the area of privacy has traditionally been left to the states to develop the appropriate balance of interests. This is consistent with the constitutional authority of the states to exercise general police powers, including legislating for the public health, safety, morals and welfare of their citizens. The result has been varied and inconsistent approaches among the states.

In each of the specific areas identified by the research into privacy laws and their impact on critical infrastructure owners and operators, issues of Federal-state relations dictate the options that are available. Federal law is only possible in those areas that touch on interstate commerce

[1] CSI/FBI 1997 Computer Security Survey.
[2] Rochelle B. Ecker, *To Catch a Thief: The Private Employer's Guide to Getting and Keeping an Honest Employee*, 63 U.M.K.C. L. REV. 251, 252 (1994).
[3] *Id.*
[4] In contrast, recent state legislation promoting the on-line availability of public records may provide more access than is needed to protect the interests of critical infrastructure employers and employers generally, to the detriment of the employee. *See, e.g.*, H.R. 2112, 55th Leg., Reg. Sess., (Washington 1997) (providing for criminal history information to be available via the Internet).

as a legal matter. As a matter of policy, Federal legislation, trumping existing state laws, may only be appropriate in those areas where the lack of uniformity among the states or failure of the states to recognize security-related issues rise to the level of national security concerns. The available approaches include:

1. **The Status Quo:** The status quo in this context amounts to a recognition and tacit acceptance of the existence and continued development of fifty very different genres of state privacy and employer-employee-related legislation.

2. **Highlighting Critical Infrastructure Issues to the States and Suggest Reconsideration of Privacy Legislation:** This is a deferential approach that will not on its own achieve uniformity, but may succeed in achieving revisions to current legislation or new legislation that is more sensitive to the needs of critical infrastructure owners and operators.

3. **Creation of a Federal Privacy Baseline:** Congress may draft and enact legislation that sets the minimum for privacy protection in a given area. States would then be free to allow for greater privacy protection as necessary. This approach, while it does articulate a Federal position, is not preemptive of state efforts (unless the state currently falls below the threshold of the Federal baseline).

4. **Federal Preemption:** In areas that touch interstate commerce, Congress may exercise its authority to pass legislation that, rather than setting a minimum which states must adhere to, completely overtakes the area of law from state control. While this is a highly intrusive approach, it creates a level uniformity across Federal and state levels that is otherwise unachievable.

5. **Study of the need for and advisability of any or all of the above approaches:** While yet another study delays action, it allows the appropriate interests to be considered and incorporated into any change, whether merely recommended to the states or mandated by Federal preemption.

These approaches may be applicable to the following areas identified as potential impediments to the achievement of infrastructure assurance objectives. These impediments tend to restrict the ability of employers, or potential employers, from screening or monitoring employees or applicants, thus constraining the ability of private owners and operators to protect critical infrastructures from insider threats by conducting the sort of background investigations routinely performed on Federal employees in sensitive positions.

Considerations for Employees in Sensitive Positions

Critical infrastructures, whether run by private sector owners and operators or the government, must utilize the services of employees. Prudence or due diligence may compel operators to explore basic questions about a current or prospective employee:[5]

- Does the employee have the necessary skills?
- Is there any background information that would militate against relying on the employee's skills?
- Is the employee honest and, does he or she possess integrity?
- Has the employee disclosed relevant job-related information, such as his or her criminal, financial, or employment history—especially background data that goes to the issue of trust, reliability, and predictability?

These inquiries are routinely made by the Federal government in screening employees for sensitive positions. The authority for these background investigations was specifically granted to the President in the Civil Service Act of 1883.[6] Federal privacy-related statutes may affect the scope of Federal background investigations. However, state privacy laws do not affect the authority of the Federal government to conduct background investigations pursuant to this Federal legislation. Without similar Congressional authorization, critical infrastructure owners and operators must observe the various Federal and state laws that govern the individual elements of employee screening. Although such inquiries may be central to an owner or operator's ability to protect critical infrastructure, Federal and state laws passed to protect personal privacy may prohibit such inquiries, or make inquiries difficult and legally suspect. In this important sense, some privacy legislation may actually serve to undercut critical infrastructure assurance.

In addition, Federal and state laws, whether statutes or common law causes of action, limit the ability and incentives for employers to share information relating to employees. For example, in 1994, an airplane crashed killing fifteen people on board. The National Transportation Safety Board concluded the cause of the crash was pilot error. Investigations revealed that before joining his current airline, the pilot had resigned from another airline to avoid being fired for failing a critical flight test. The airlines did not share that information. In fact, most airlines have specific

[5] Fear of tort liability may also prompt employers to conduct background investigations. *See* discussion *infra* p. 15 of "negligent hiring."

[6] Currently codified at 5 U.S.C. § 3301 (1997). This authority is implemented by Exec. Order 10450, Civil Service Investigations.

policies in place preventing sharing of that type of information to avoid liability from suit.[7] The fear of liability, whether or not it is justified, operates in many instances to prevent adequate screening of potential employees or sharing of information about prospective employees.

Relevant Law and Legislation

The following types of state laws may present infrastructure assurance issues:

Criminal History Information

The criminal history of a prospective employee, or information on any subsequent arrests or convictions once hired, is an important tool used by employers in determining the suitability of an individual to a sensitive position. As a legal matter, obtaining criminal history information is primarily governed by state law. States regulate the collection and maintenance of criminal justice record systems and the rules under which such information may be made available to individuals and third parties. State laws regarding civil rights, employment, or (in the case of New York state) corrections, set out the rights of applicants and employers with respect to requesting and reviewing criminal history information. In addition, both Federal and state equal employment laws provide guides for the proper use of criminal history information in hiring decisions. It is important for purposes of employment issues to maintain a crisp distinction between information disclosing a *conviction* and information reporting a mere *arrest*. While arrest information may be available through state means, Federal law strictly prohibits potential employers from requesting such information or using the information in making hiring decisions.

Access to Criminal History Records

Criminal history information is maintained both by the Federal and state governments. According to the rules set out at 28 C.F.R. § 20.1 *et seq*., the Federal Bureau of Investigation administers the National Criminal Information Center (NCIC). States may receive funds and participate in the NCIC if willing to conform to the regulations governing the database. Individuals may request and review their NCIC records to verify their accuracy. Federal regulations place substantial restrictions on the availability of arrest (without conviction) information, but allow states full discretion to permit access to conviction information by third

[7] Robert Adler & Ellen Pierce, *Encouraging Employers to Abandon Their "No Comment" Policies Regarding Job References: A Reform Proposal*, 53 WASH. & LEE L. REV. 1381, 1383 (1996).

parties. In fact, the regulations specifically recognize the public nature of much of the criminal history information related to convictions and does not regulate that information to the extent it is available from an independent source (i.e., other than the centralized state criminal information system or the NCIC). Federal officials, through the FBI, will only release criminal history information for employment purposes to requesting third parties who are banks, state and local governments, registered securities exchanges or nuclear power providers.[8]

If a state does not participate in the NCIC, they are free to regulate their centralized criminal history information system as they choose. In addition, to the extent that they do participate, states may still regulate access to conviction information by third parties. Some states, such as Colorado, have taken a liberal approach to the availability of such information allowing complete access to criminal history information except for the names of victims of sexual offenses. Delaware releases conviction information of job applicants and employees to employers directly without any requirement of employee consent.[9] Other states limit the information available to third parties to information relating to convictions within a certain time frame.[10] As a general rule, individuals have access to their criminal history records at state and Federal levels.[11] Records may, in some instances, also be released to a third party based on the individual's consent.[12] Only a few states do not allow copies of criminal history records to be released to individuals or their agents.[13]

Employer Inquiries into Criminal History

A more contentious issue than simply the availability of criminal history records, is employer inquiries into criminal histories as part of a hiring process. At the Federal and state levels, this is regulated as a matter of fair employment and civil rights practices. Both the Federal government and 41 states prohibit requests for *arrest* information.[14] Some states do allow inquiries into current arrests and pending criminal matters. States have set additional limitations on inquiries relating to criminal backgrounds. Massachusetts, for example, prohibits questions relating to misdemeanor convictions.[15] Still other states set time limitations to allow access only to "current" offenders. Other states only allow inquiries into criminal histories for certain

[8] *See* 28 C.F.R. §§ 20.33 & 50.12.
[9] DEL. CODE ANN. tit. 11, § 8513(c)(1) (1996).
[10] *See, e.g.,* ALASKA STAT. § 12.62.160 (1996).
[11] *See, e.g.,* ARK. CODE ANN. §§ 12-12-211 through 12-12-213 (1995 Repl. Vol.); CAL. PENAL CODE § 13323 (1996); GA. CODE ANN. § 35-3-34 - 35-3-37 (Supp. 1996).
[12] *See, e.g.,* KAN. STAT. ANN. § 22-4710 (1996) (employer access to criminal history based on signed release by applicant).
[13] *See, e.g.,* LA. REV. STAT. ANN. § 15:588 (West 1996); MINN. STAT. ANN. § 13.87 (West 1996) (allows any member of the public to view criminal history information on a computer monitor); MISS. CODE ANN. § 45-27-11 (1996) (copy of record only available to individual or their attorney if contesting information therein).
[14] *See* Commission Decision No. 74-02, CCH EEOC Decision (1973); Rochelle B. Ecker, *To Catch a Thief: The Private Employer's Guide to Getting and Keeping an Honest Employee,* 63 U.M.K.C. L. REV. 251, 255 (1994). Inquiring about arrest histories has been determined to be employment discrimination in violation of Title VII of the Civil Rights Act of 1964 on a theory of disparate impact. Disparate impact is generally applicable when a criterion, while neutral on its face, has a statistically greater impact on one segment of the population than others.
[15] *See, e.g.,* MASS. GEN. LAWS ANN. ch. 151B, § 4(9) (1991).

statutorily enumerated job positions, usually involving the supervision of minors (e.g., teachers, day care operators, etc.). The California Penal Code prohibits employers from requiring applicants to provide a copy of their criminal records.[16] As a general rule, inquiries regarding *convictions* are permissible to the extent job-related.

Use of Past Convictions in the Hiring Decision

Even more controversial than access to or inquiries into criminal histories are the uses of such information by an employer in making a hiring decision. In general, both as a matter of Federal and state law, employers may take conviction information into account, to the extent it is available (see above), in the hiring process provided the employer considers: (1) the seriousness of the offense or offenses; (2) the age of the person at the time of the offense; (3) the time which has elapsed since the offense or offenses; and (4) the bearing the conviction of such an offense has on the ability of the individual to perform the duties or responsibilities of the position for which they applied.[17]

While such considerations should be taken into account by infrastructure owners and operators, in the vast majority of cases, individuals, particularly those in sensitive positions, may be screened for criminal convictions. And the closer the relationship to public safety (which in the critical infrastructures is often a very close nexus), the greater the assurance of the employer that they will not be subjected to liability for violations of employment-related laws. However, care must still be given to properly observe the state law requirements with regard to use of criminal conviction information. Some states do require written explanations of the grounds for denying an applicant a position based on criminal history.

Credit History Information

Availability of credit history information is governed primarily by the Federal Fair Credit Reporting Act (FCRA).[18] The FCRA sets out rules for requesting and receiving information, procedures for use of the information in making hiring decisions, and provisions for applicants to seek recourse for inaccurate and damaging information. Individuals may request and receive information concerning their own credit history from credit bureaus. In addition, employers may directly, and with no requirement of applicant consent, request and receive credit history information from credit bureaus as long as they are using the information to make employment decisions.[19] If an applicant is not hired based on information contained in their credit report, they must be notified of the reason in writing with the name and address of the credit reporting agency. Applicants can then request the information and review it for discrepancies. Procedures

[16] CAL. PENAL CODE § 13326 (1996).
[17] *See, e.g.,* N.Y. CORRECTION LAW § 753 (McKinney 1997).
[18] 15 U.S.C. §§ 1681-1681t (1996).
[19] 15 U.S.C. § 1681b.

are in place for disputing information contained in credit reports. This framework established by the FCRA is the model for much of the state legislation in the area.[20] In fact, to the extent any state law is inconsistent with the Federal provisions in the FCRA, the state law is preempted.

Polygraph Examinations

Federal and state laws limit the use of polygraph testing by employees, including the owners and operators of critical infrastructures. Federal law does not apply to state and local governments; absent state legislation, there is no general prohibition against use for state and local government employees.

State Law

The need for Federal polygraph protection surfaced in the 1980s after employers forced polygraph testing on unsuspecting employees in record numbers, often circumventing state laws to protect employees. In the early part of the 1980s, employee theft resulted in losses ranging from $9.2 billion to $50 billion per year.[21] Employers responded with over two million polygraph tests annually to screen job applicants, investigate specific incidents of theft, and to uncover employee misconduct.[22] Forty-one state legislatures responded with legislation after employees protested that the examinations were unduly intrusive and did not detect deception.[23] However, because the state laws lacked uniformity, employers were able to force employees to submit to tests in neighboring states, where laws were relatively lax.

Federal Law

Congress responded by passing strong Federal legislation. The Employee Polygraph Protection Act (EPPA)[24] makes it unlawful for an employer "directly or indirectly, to require, request, suggest, or cause any employee or prospective employee to take or submit to any lie detector test."[25] Violations may be punished by a civil penalty of up to $10,000.[26] The Act specifically identifies: who may be asked to take a polygraph; for what purpose or limited set of positions it

[20] *See, e.g.*, ARIZ. REV. STAT. ANN. § 44-1691 through 1696 (1996); CAL. CIVIL CODE §§ 1785-1786.56 (1996); KAN. STAT. ANN. §§ 50-701 through 722 (1996); MASS. GEN. LAWS ANN. ch. 93 §§ 50-68 (1997); N.M. STAT. ANN. §§ 56-3-1 through 56-3-8 (1997).

[21] *See* C. Cullen, The Specific Incident Exemption of the Employee Polygraph Protection Act: Deceptively Straightforward, 65 NOTRE DAME L. REV. 262 (1990).

[22] *Id*., *citing to* Privacy Protection Study Commission, Personal Privacy in an Information Society (1977) at n.. 7 (reporting that in 1977, by contrast, only 300,00 lie detector tests were given).

[23] *See id*. at 263-264. For an excellent summary of the Act, please refer to L. Pincus and C. Trotter, *The Disparity Between Public and Private Sector Employee Privacy Protections: A Call for Legitimate Privacy Rights For Private Sector Workers*, 33 AM. BUS. LAW JOURNAL, 50, 68-70 (1995) (hereinafter "Employee Protections").

[24] 29 U.S.C. §§ 2001 - 2009; Pub. L. No. 100-347, 102 Stat. 646.

[25] 29 U.S.C. § 2002.

[26] 29 U.S.C. § 2005.

may be requested; the types of questions employers may ask in polygraph testing; the allowable uses of the results; and whether the results may be disseminated.

According to the Act, information obtained from the polygraph examination cannot be disclosed except to the examinee, the employer requesting the test, courts or agencies pursuant to a court order.[27] The Act includes several major exemptions to the general rule that no one may be subject to a polygraph test. With respect to the critical infrastructures, these exemptions are significant, and include: all Federal, state, local governments and employees;[28] certain DOD, DOE, intelligence community and FBI contractors and employees.[29] Exemptions also appear for employers to use testing as a tool in ongoing employment-related investigations, which require the employer to show reasonable suspicion and follow carefully delineated investigative procedures.[30]

Exemptions written into the Act carve out several areas where employers may continue to use the polygraph.[31] One pertinent exception applies to employers who provide security-related services. For these employers, polygraph testing for applicants and existing employees is permitted. This exemption covers employers (1) whose primary business purpose consists of providing security, such as armored car personnel, personnel who install or maintain alarm systems, or other uniform or plainclothes security personnel; *and* (2) whose function includes protection of facilities, materials, or operations having a significant impact on the health or safety of any State or political subdivision, including electric power plants, public water supply systems, public transportation, and the protection of currency, negotiable securities, precious commodities or proprietary information.[32] The exemption appears to extend to a wide range of *physical* security services, but its application to those who provide *information* security services remains unclear. Likewise, providers of telecommunications services are not included in the enumeration of protected facilities.

The Department of Labor's implementing regulations elaborate on this exemption. According to the regulations, both of these preconditions must be met for the employer to claim an exemption.[33] That is, the employer must be primarily in the business of protecting the facilities and the facilities may be publicly or privately owned, and may be construed broadly to include a wide range of infrastructure facilities.[34]

[27] 29 U.S.C. §§2006 - 2008; 29 C.F.R. §§ 801, 801.10 - 801.14 (1997).
[28] 29 U.S.C. § 2006 (1988), 29 C.F.R. § 801.10 (1997). States may choose, however, to pass more restrictive polygraph legislation. The Act also would not preempt a more restrictive collective bargaining agreement provision.
[29] 29 U.S.C. § 2006e; 29 C.F.R. §§ 801.11 - 801.14 (1997) (Department of Labor regulations construing EPPA).
[30] *Id*.
[31] 29 U.S.C. § 2006(e)(1)(A)(i) - (iv); s*ee also* 29 C.F.R. Part 801, 801.10 - 801.14 (1997).
[32] *Id*. at 29 U.S.C. § 2006(e)(1).
[33] 29 C.F.R. § 801.14(c)-(d)(1) (1997).
[34] *Id*. ("… These examples are intended to be illustrative, and not exhaustive.") *Id*.

Interaction of State and Federal Law

It is important to note that the EPPA does not completely preempt state law on the use of polygraph tests. The EPPA does govern exclusively the exemptions allowing use of polygraph tests by government employers (Federal, state and local), for national defense and security reasons by the Federal government, and of FBI contractors.[35] The EPPA also sets a minimum level of protection for private-sector employees in all states. That is, states must observe the prohibition on use of polygraph tests set out in the EPPA, however, they may refuse to accept the exceptions to the prohibition recognized in Federal law, or craft more narrow ones. To the extent a state law is more restrictive than the Federal law, it will control in an employment matter in that state. For this reason, exemptions must be considered on a state by state basis. The result being that any modification to the Federal exemptions that broaden their scope may be of limited effect alone. Unless they are included among the preemptive provisions of the Act, or states opt to recognize the need for broader exemptions, they will not have wide application outside of Federal issues. Select state exemptions are highlighted in the table, below.

State	Polygraph law
Alaska	General rule is to prohibit; exemptions for law enforcement. Alaska Stat. § 23.10.037(a).
California	General rule is to prohibit; exemptions for government officials. Cal. Labor Code § 432.2 (West 1989) (Lie-Detector Testing).
District of Columbia	General rule is to prohibit; exemptions for criminal investigation by Metro police or fire departments, or Department of Corrections.
Kansas	Repealed 1989 law (Kan. Stat. Ann. § 75-744 (1989).
Maine	Pre-employment: General rule is to prohibit. Current employees: General rule is to prohibit. Exemptions for law enforcement. Employee can voluntarily submit.
Minnesota	General rule is to prohibit. If one is given, results can only be given to employee and persons authorized by employee to receive results.
Montana	General rule is to prohibit; exemptions in areas of "security", "public safety" and where there is a "fiduciary responsibility."
New York	General rule is to prohibit.
Pennsylvania	General rule is to prohibit. Exemptions for law enforcement or who dispense narcotics and dangerous drugs.

[35] 29 U.S.C. §§ 2006 & 2009.

Employment History

Personnel records often contain details of an individual's employment history, such as reprimands or disciplinary actions, that could have a bearing on their fitness for a sensitive position within a critical infrastructure. Depending on whether an employer is Federal government, state government or private, a different set of rules governing access to employment records applies (*e.g.*, Federal and state Freedom of Information Acts). However, a few generalizations can be made. Employers are generally required to ensure the accuracy of the records they keep and to allow employees an opportunity to review the records to verify the information they contain. Provisions for inspection of personnel records are included in the Federal Privacy Act (which applies only to information held by the Federal government) and in various state statutes.[36] These records may be released to third parties only with the consent of the employee they concern or pursuant to advanced written notice.[37] Employers may not share employee personnel records with each other without the involvement of the employee.

Defamation as a Limit on Disclosure

In addition to the specific statutory limits on dissemination of information in employment records, there are also tort-based laws which may prevent employers from sharing relevant information. These tort laws are state level statutory or common law creations. They protect individuals from invasions of privacy and damage to reputation to varying degrees. To the extent this issue is governed primarily by case law rather than statutes, the individual predilections of judges and juries contribute to immense diversity among the states in possible acts that could create liability for an employer. Although other causes of action are available, defamation has most recently been invoked with regard to unfavorable references. Defamation is the publication of anything injurious to the good name or reputation of another, or which tends to bring him into disrepute.[38] A common, modern day dilemma exists for all employers who are called to discuss a former employee. What can the employer say if the employee's performance was poor? What if the employee was let go for a suspected theft? If a critical infrastructure facility is hiring for a sensitive position, can it seek and obtain accurate references on a job applicant?

Defamation is handled predominantly in state legislatures or the courts. Most states have handled defamation in widely different ways. Many states recognize defenses, such as "truth" and "employer immunity." Certain generalizations can be made, such as:

- *Truth* is always a defense to the common law claim of defamation;

[36] *See* 5 U.S.C. § 552a(d); *see, e.g.*, CONN. GEN. STAT. § 31-128f (1997); D.C. CODE ANN. § 1-632.5 (1997); MICH. COMP. LAWS § 423.506 (1997); OR. REV. STAT. § 652.750 (1997); WIS. STAT. § 103.13 (1997).
[37] *Id.*
[38] *Western Union Telephone Co. v. Lesesne*, 198 F.2d 154 (4th Cir. 1952) (prima facie case defined).

- *Qualified privilege* is used if it is a true statement made in good faith serving a business interest or purpose. A harmed employee can defeat a qualified privilege by showing malice—actual knowledge of falsity or reckless disregard for the truth.

- Some states allow for employer immunity where information is offered in good faith (see chart below).[39]

State	Approach to Defamation
Idaho	An employer who in good faith provides information about the job performance, professional conduct, or evaluation of a former or current employee to a prospective employer of that employee, at the request of the prospective employer of that employee, or at the request of the current or former employee, may not be held civilly liable for the disclosure or the consequences of providing the information. Idaho Code § 44-201 (Employer Duties).
Maine	26 M.R.S.A. § 598 MAINE REVISED STATUTES ANNOTATED TITLE 26. LABOR AND INDUSTRY CHAPTER 7. EMPLOYMENT PRACTICES SUBCHAPTER I. CONDITIONS FOR EMPLOYMENT § 598. Employment reference immunity An employer who discloses information about a former employee's job performance or work record to a prospective employer is presumed to be acting in good faith and, unless lack of good faith is shown by clear and convincing evidence, is immune from civil liability for such disclosure or its consequences. Clear and convincing evidence of lack of good faith means evidence that clearly shows the knowing disclosure, with malicious intent, of false or deliberately misleading information. This section is supplemental to and not in derogation of any claims available to the former employee that exist under state law and any protections that are already afforded employers under state law.

[39] *See, e.g.*, Florida, Delaware, and Kansas have also recently passed employer immunity statutes. *See* FLA. STAT. ANN. § 768.095 (West 1997) (employer immunity from liability); KANS. STAT. ANN. § 44-119(a) (Supp. 1996) (immunity from liability); DEL. CODE ANN. Tit. 19, § 708 (Supp. 1996) (immunity for employer). *See also* D. Scott Landry & Randy Hoffman, *Walking the Fine Line on Employee Job Reference Information*, 43 LA.B.J. 457 (1996). (Law review article on trend in South for employer immunity).

Indiana	§ 22-5-3-1 Disclosure of information after employee's discharge Sec. 1. (a) A person who, after having discharged any employee from his service, prevents the discharged employee from obtaining employment with any other person commits a Class C infraction and is liable in penal damages to the discharged employee to be recovered by civil action; but this subsection does not prohibit a person from informing, in writing, any other person to whom the discharged employee has applied for employment a truthful statement of the reasons for the discharge. (b) An employer that discloses information about a current or former employee is immune from civil liability for the disclosure and the consequences proximately caused by the disclosure, unless it is proven by a preponderance of the evidence that the information disclosed was known to be false at the time the disclosure was made. (c) Upon written request by the prospective employee, the prospective employer will provide copies of any written communications from current or former employers that may affect the employee's possibility of employment with the prospective employer. The request must be received by the prospective employer not later than thirty (30) days after the application for employment is made to the prospective employer.
Louisiana	LSA-R.S. 23:291 § 291. Disclosure of employment related information; presumptions; causes of action; definitions A. Any employer that, upon request by a prospective employer or a current or former employee, provides accurate information about a current or former employee's job performance or reasons for separation shall be immune from civil liability and other consequences of such disclosure provided such employer is not acting in bad faith. An employer shall be considered to be acting in bad faith only if it can be shown by a preponderance of the evidence that the information disclosed was knowingly false and deliberately misleading. B. Any prospective employer who reasonably relies on information pertaining to an employee's job performance or reasons for separation, disclosed by a former employer, shall be immune from civil liability including liability for negligent hiring, negligent retention, and other causes of action related to the hiring of said employee, based upon such reasonable reliance, unless further investigation, including but not limited to a criminal background check, is required by law.

	C. As used in this Section, the following words and phrases shall have the meanings contained herein unless the context clearly requires otherwise: (1) "Employer" means any person, firm, or corporation, including the state and its political subdivisions, and their agents, that has one or more employees, or individuals performing services under any contract of hire or service, expressed or implied, oral or written. (2) "Employee" means any person, paid or unpaid, in the service of an employer. (3) "Prospective employer" means any "employer", as defined herein, to which a prospective employee has made application, either oral or written, or forwarded a resume or other correspondence expressing an interest in employment. (4) "Prospective employee" means any person who has made an application, either oral or written, or has sent a resume or other correspondence indicating an interest in employment. (5) "Job performance" includes, but is not limited to, attendance, attitude, awards, demotions, duties, effort, evaluations, knowledge, skills, promotions, and disciplinary actions.

Despite the availability of defenses and the likelihood they may prevail in a civil suit, many employers are nonetheless reluctant to do anything more than verify dates of employment, salaries and other factual information. Some states have recently enacted legislation expanding immunity from civil suits for employers who provide references in good faith. Prior to 1995 only five states had such statutes. By October of 1995, nine more states had enacted such legislation. Louisiana passed similar legislation in 1996.[40] The momentum of these legislative initiatives may increase due to other emerging civil actions relating to employee hiring.

There is an additional incentive to share information about employees. As of 1991, 30 states, including California, recognized the tort of negligent hiring. In determining whether the tort of negligent hiring has been committed, "courts look to whether the employer reasonably investigated the employee's background before hiring the employee."[41] Access to information about prospective employees is important to all employers, if for no other reason than to avoid this type of liability. The current state of tort law with regard to employee references truly demonstrates the complexity of the interests at stake in the employer-employee relationship and the difficulty of balancing those equities.

[40] 43 LA. B.J. at n.3.

[41] Janet Swerdlow, *Negligent Referral: A Potential Theory for Employer Liability*, 64 S. CAL. L. REV. 1645, 1646 (1991) (in the article, the author advocates the creation of a tort law duty of employers to provide accurate and substantive references on former employees).

Part Three

Approaches For Addressing Privacy Issues

General Recommendation By The Federal Government That States Individually Examine Potential Unintended Consequences Of Related Legislation And Consider Benefits Of Adopting Unified Approaches

Without enacting any particular approach, Congress or the Administration could acknowledge the importance of *certain* employers being permitted to gather *certain* types of job-related information for *certain* sensitive positions, and the difficulties and unpredictability brought about through multiple state approaches. The Federal government could suggest that states clarify their own laws regarding the types of records and information employers may acquire, for what positions, and under what circumstances. In this way, the Federal government can influence state legislatures to revisit the impact of their own laws in light of infrastructure assurance objectives. Critical infrastructure owners and operators can be encouraged to lobby state legislatures to incorporate specific exemptions in these privacy provisions—thereby allowing more careful screening of applicants for sensitive positions. Additional measures may include Federally-directed awareness campaigns at state legislatures and private industry executives to raise awareness of infrastructure assurance issues relating to employee security.

- **Pro:** Allows Federal government to "air views" while demonstrating maximum deference to states. Minimally intrusive approach impinges neither upon individual privacy concerns nor state sovereignty or federalism concerns, but encourages long-term conformity to infrastructure assurance objectives. Allows each state legislature to determine the balance between privacy and security concerns *for that state*.

- **Con:** Unlikely to result in meaningful change absent more specific guidance backed by statute or regulation. Retains geographical differences between laws governing electronic data transmissions — resulting in lack of uniformity between the states with respect to "rules of the road" for information conveyed across state lines. Difficulty of achieving compliance with laws across more than 50 different jurisdictions may discourage owners and operators from seeking information they might otherwise be entitled to receive. Leaves legislative "spadework" to infrastructure owners and operators -- but they are unlikely to rally at state and local levels for what may be perceived as an unpopular cause.

Federal Government Points Out Benefits Of States Voluntarily Adopting Minimal Consensual "Baseline" For Acquisition Of Background Information, At Least For Owners And Operators Of Critical Infrastructures

Congress and the Administration can acknowledge the importance of allowing critical infrastructure owners and operators to acquire sensitive background information for certain employment positions through consent of the employee or applicant. Assuring nationwide availability of a consensual "baseline" would represent a reasonable compromise between employees' privacy concerns and the security needs of owners and operators of critical infrastructures. This approach would allow implementation by the states in a narrow or broad manner — they could make legitimate, job-related information available to a broad or narrow class of employers, for a broad or narrow set of positions.

- **Pro:** This approach is minimally intrusive as most of the states already achieve this "baseline" under current law. Recognizes benefits of uniformity and importance of screening for employees in sensitive positions in critical infrastructures, while allowing state lawmakers to achieve balance based on regional values. Such an approach would allow the Federal government to point to the benefits of a predictable nationwide climate governing employer-employee relationships in this area, particularly where electronic record checks could one day be the norm.

- **Con:** Will fail to achieve uniformity.

The Administration Can Name A Panel To Consider Best Approach To Achieving Legislative Balance Between Security Needs And Privacy Interests

The Administration can form a study panel constituted to adequately represent Federal, state, and local government interests, as well as private sector representatives of labor and management, to consider a balance between security needs and privacy interests. The study panel can be tasked to consider, among other things, some of the concerns and equities raised in this paper (e.g., balance between privacy and security concerns, employee and employer equities, and state and Federal interests). The balance they strike may be reflected in form of a general statement of objectives, or perhaps a model privacy statute or uniform law for states to consider. They may decide to issue a call for partially or wholly preemptive Federal legislation.

- **Pro:** Relatively unintrusive process, can be implemented with limited resources. Promotes open and balanced dialogue between numerous interested parties, and implementation by legal experts. Enhances awareness and broadens participation in the process. Allows careful consideration and crafting of recommendations.
- **Con:** Defers serious resolution of the issue indefinitely.

Congress And The Administration Can Recommend Narrow Amendments To *Federal* Privacy Laws To Serve As Model For State Legislative Reform

The Federal government can identify potential security-privacy shortfalls in existing Federal legislation and recommend modest changes while at the same time demonstrating to state

legislatures and owner-operators some of the benefits to be derived from reconsideration of legislation in light of infrastructure assurance objectives.

- **Pro:** Offers specific guidance to Congress to promote immediate action and discussion without need to await findings of study group. Offers useful example to states while at the same time respecting comity concerns.

- **Con:** Unlikely, on its own, to enhance uniformity. Could even promote further diversity by encouraging individualized state approaches.

The Administration Can Recommend Limited Congressional Preemption Of State Privacy Laws To Accommodate Data Collection Needs

The Administration can recommend that Congress consider the propriety of establishing a mandatory information collection and dissemination "baseline" with which relevant state privacy legislation must comport, thereby assuring owners and operators the ability to perform the equivalent of "background checks" on employees or prospective employees occupying certain sensitive positions. This might be accomplished, for example, through Congressional findings equating certain positions of employment within the critical infrastructures with Federal government positions that require security clearances.

- **Pro:** This approach would set a standard for privacy across all fifty states at the level required for infrastructure protection. It would tend to unify existing practices thus increasing predictability for business.

- **Con:** Congressional support is unpredictable if not unlikely. It is not clear that infrastructure owners and operators would be willing to shoulder additional expense associated with background checks absent subsidies or incentives unless they were in their own vested business interests. This approach may be polarizing in new and unfamiliar ways.

Part Four

Conclusions

Employers have a valid interest in acquiring information about current and prospective employees. This is certainly true of owners and operators of critical infrastructures—particularly with respect to employment in certain sensitive positions. Recently, however, the prevailing concerns of state and Federal lawmakers has been to solidify other valuable intereststhose of employee privacy. And while the Federal government has been the traditional arbiter of concerns relating to the national security, concerns relating to individual privacy are the traditional province of the States. The Administration and Congress should proceed cautiously to insure that a proper balance is struck between security and privacy concerns, a balance respecting the authority of the Federal and state governments. One way to achieve such a balance may be to allow greater employer access to job-related background information (criminal history, credit, past employment) for specific types of positions, while also ensuring that appropriate procedures are in place to allow employees to be certain of the accuracy and fair use of such information.

Diversity of State and Federal Law

A diversity of interests have given rise to varied state and Federal approaches to the acquisition and use of personal information for employment purposes (e.g., criminal history, credit, employment). These approaches often reflect regional values—but have resulted in a disparate framework for the nation. This creates complications for employers whose own operations may span several jurisdictions, or who may wish to inquire about employees who have themselves lived in a number of states. It is not vital to advocate resolution of these uncertainties for all employers and all job positions. Rather, the Federal government should only seek to make predictable procedures available for employers seeking to fill positions of high sensitivity within the critical infrastructures.

Insider Threats to the Critical Infrastructures

The Federal government recognizes that insofar as the critical infrastructures may provide attractive targets to physical and cyber attack, the owners and operators and their employees may be, in some instances, the first and only line of defense. This fact suggests that some of the positions held within the critical infrastructures may be relevant if not vital to national security. The Federal government would not likely fill a position of such gravity without conducting a background investigation, and would likely keep that information current. Some owners and operators of critical infrastructures, however, are prevented by the operation of state and Federal laws from taking analogous protective measures. Impediments to background inquiries have been put in place in the service of other interests—privacy, fair employment, post-conviction rehabilitation—without necessarily having taken into account the relatively novel concerns of infrastructure assurance. Similarly, the exemptions to those impediments are legislative responses to a different though often related set of concerns. Infrastructure assurance objectives may be achieved in some instances through minor modifications to the exemptions.

Employee Screening Procedures

The current practice of the Federal government is to conduct routine reinvestigations into employee backgrounds at regular intervals after the initial screening for many of its sensitive employment positions. General baseline principles for collecting and using criminal history, credit, polygraph and other types of information identified here can apply equally to initial hiring as well as to the subsequent "updating" of relevant, job-related information on an employee.

Such conclusions do not represent a mandate or endorsement of any particular employee screening or reinvestigation practice. It is far better to establish a consensual baseline between *certain* employers and *certain* applicants for sensitive employment. This baseline would serve to merely make available to a potential or current employer relevant job-related information, to be used in a manner consistent with prevailing law, upon consent of the applicant.

Fair Information Practices

It is very important to observe fair information practices in any aspect of these issues bearing on privacy and information sharing.[42] Fair information practices are at the foundation of Federal legislation such as the Fair Credit Reporting Act and the Privacy Act of 1974. Fair information practices are principles for collection, use and dissemination of information which should be considered by both Federal and state governments when drafting laws dealing with personal information.

Advocating a "Consensual Baseline" Approach

It may be appropriate to raise to state legislatures and to Congress the possibility that existing privacy laws may unduly hinder attempts by certain employers to take legitimate security precautions—precautions that may otherwise be justified in light of national security and economic concerns. Ideally, lawmakers would want to reexamine existing legislation and take into account these security concerns in the future. Naturally, careful consideration of all of the interests at stake should be given before striking an appropriate balance of those interests in law. Consideration should also be given to the benefits of uniformity among the states in this area.

Under such circumstances, an appropriate "baseline" might be constructed around employer-employee consent, whereby an applicant for certain sensitive positions within the critical infrastructures might grant, upon request, third party access to documents (under conditions that reflect fair information practices). This is an approach currently in place in several states, but a

[42] Fair information practices are a set of global principles that define fair procedures for the collection and use of personal information. Personal information is any information that can be associated with an identifiable individual. These principles are the basis for all federal privacy laws and are reflected in the Clinton Administration policies for the Global Information Infrastructure. Fair information practices include the following principles:

- The information collected should be clearly relevant to the purpose for which it is being collected;
- People must be able to learn what personal information is in their records and how the information is being used. There should be no secret systems;
- People must be able to inspect their records and correct any errors;
- Personal information should not be collected for one purpose and used for other purposes without the individual's knowledge and consent; and

Organizations that create, maintain, use or disseminate records containing personal information must assure the reliability of the information for its intended use and must ensure that the information is protected against misuse. Fair Information Practices were developed in 1973 by a Advisory Committee to the Department of Health, Education & Welfare (now HHS), chaired by Dr. Willis Ware.

few states do not allow for individuals—much less third parties—to obtain copies of certain types of information. As a first step, states should allow individuals to obtain copies of their records and allow employers to request that employees provide relevant information when applying for certain sensitive positions within the critical infrastructures.

Privacy-Security Study Group

A baseline of consent across U.S. jurisdictions will provide a degree of uniformity and consistency currently absent from employee screening laws. But this paper does not account for the role of labor unions and collective bargaining, the trend toward increased availability of personal information via the Internet, nor many of the other practical, financial or legal issues involved in the employee-employer relationship. A comprehensive study of these issues would best be performed by a study body of relevant professionals—lawyers; labor and management representatives; privacy advocates; Federal, state and local government representatives. They could explore the issues identified in greater depth in order to make findings and recommendations for the further modification of Federal and state legal regimes governing this area.

Ideally, the Attorney General could be directed to convene such a study group charged to address, among other related issues, the following:

- Identify current Federal and state legislation that may impede owners and operators of critical infrastructures from obtaining job-related background information on job applicants and current employees for sensitive positions (under conditions similar to those by which, for example, the Federal government obtains information before issuing security clearances);

- Identify other potential impediments to a private background investigation process (e.g., practical difficulties in obtaining criminal history information, financial issues, influence of collective bargaining agreements, etc.);

- Identify individual privacy and civil liberties issues implicated by a private background investigation process and existing legal protections for those interests;

- Analyze whether there are gaps in authority with respect to availability, collection, or dissemination of information relevant to an employee's suitability for a sensitive position, or protection of personal privacy interests that should be filled by legislation;

- Analyze the current tort litigation climate and its influence on employer-employee relations taking into account recent trends in legislation;

- Make recommendations to enable a private background investigation process that strike the appropriate balance between all of the stakeholders, taking into account:

    - federalism concerns;
    - privacy interests;
    - civil rights/fair employment practices;
    - labor law;
    - tort liability;
    - fair information practices;
    - financial issues and other practical impediments.

- Specifically delineate the infrastructures and positions to which such recommendations may apply;

- Consider the propriety of producing model state legislation, or (if perceived as necessary under the circumstances) partially preemptive Federal legislation reflecting vital national security interests.

Illustrative Amendments to Federal Legislation

Given an adequate opportunity to review all the laws that are implicated by this issue, fairly specific recommendations for legislative reform may follow. But more modest changes can bring some degree of relief, and can illustrate the benefits of reconsidering prevailing laws in light of infrastructure assurance objectives. One statute in particular represents an example of the type of change a study body may suggest. This statute is the Employee Polygraph Protection Act (EPPA). The EPPA broadly prohibits private employers from subjecting employees to polygraph examinations. The statute also provides, however, some narrow exemptions. Included in the exemptions are employers who are in the business of providing security services for the protection of certain types of enumerated facilities, many of which are part of critical infrastructures.

In fact the current Department of Labor regulations implementing the EPPA appear to include all of the critical infrastructures within the scope of the exemption.[43] Through the operation of this exemption, for example, employers who provide employees to install alarm systems at electric power facilities may administer polygraphs to those employees under the limited conditions

[43] See 29 C.F.R. Part 801.

described in the Act. Interestingly, however, under current wording, an employer responsible for providing analogous "cyber" security services—such as the installation of firewalls or other protective technologies—appears not to be able to take similar precautions.

Research to date has shown that some distinctions—such as those between physical and information security—often break down where infrastructures are highly interdependent and where threats can be physical, cyber or both. Amendments could be made to the EPPA to include within the scope of its exemptions those who are in the business of providing information security services. (*See* Appendix A). Such amendments do not make it incumbent upon covered employers to polygraph employees, but merely allows them to do so to the extent permitted under applicable state law.[44]

The insider threat is as important an issue as it is difficult to address. It is important to emphasize the importance of linking these efforts to other efforts, such as international policies, standards, and training and education, which also may touch on potential problems arising from an unfortunate but potentially significant insider threat.

[44] The proposed amendments shown in Appendix A would include under the EPPA's exemptions most of the critical infrastructures and would also be an important step in amending extant legislation to reflect the growing importance of information security alongside physical security. However, the potential limitations to the effectiveness of such a revision further indicate the need for a careful study of these issues. The EPPA provides only limited preemption of state legislation. States remain free to create more restrictive exemptions and thus broadening the federal exemptions may leave state coverage unchanged. Nonetheless, the EPPA affords an important opportunity for Congress to demonstrate to state lawmakers its concern over information security, particularly as implemented within the critical infrastructures.

Appendix A

Proposed Amendment to EPPA

[Summary of 29 U.S.C. 2001-2009; Employee Polygraph Protection Act, incorporating proposed revisions to section 2006(e).]

Section 2001. Definitions

Section 2001 defines "lie detector" to include a "polygraph, deceptograph, voice stress analyzer, psychological stress evaluator, or any similar device (whether mechanical or electrical) that is used . . . [to] render a diagnostic opinion regarding the honesty or dishonesty of an individual."

Section 2002. Prohibitions on lie detector use

Section 2002 makes it unlawful for any employer in interstate commerce to (1) "require, request, suggest or cause" an employee or prospective employee to take or submit to a lie detector test; (2) to "use, accept, refer to or inquire concerning" the results of "any lie detector test of any employee or prospective employee"; (3) to discharge, discipline or otherwise discriminate against an employee or prospective employee for refusing to take the test or on the basis of the results of such a test; or (4) to discharge, discipline or otherwise discriminate against an employee or prospective employee for exercising rights under this section.

Section 2003. Notice of protection

Section 2003 requires the Secretary of Labor to produce and distribute, and for employers to post, summaries of the pertinent provisions of this chapter in conspicuous places.

Section 2005. Enforcement provisions

Section 2005 allows the Secretary of Labor to assess penalties of up to $10,000. The Secretary may bring suit to restrain violations. This provision also permits employees a private right of action to recover damages and seek reinstatement. It expressly disallows employee waiver of any of the provisions of the chapter.

Section 2006. Exemptions

Section 2006 makes the chapter inapplicable to (a) federal, state or local government employees, and to (b) certain DoD, DOE, intelligence community, and FBI contractors. It also *permits* an employer to ask an employee to submit to an examination if it is offered (d)(1) in connection with an ongoing investigation; (d)(2) if the employee had access to the property that is the subject of the investigation; (d)(3) if the employer reasonably suspects the employee was involved; and (d)(4) the employer complies with procedural requirements, such as providing prior written and signed notice of the offense under investigation, an estimation of the resulting loss or damage, and a statement describing the basis of the employer's reasonable suspicion.

Section 2006(e) contains an exemption for providers of security services

* * * * *

e) Exemption for security services

(1) In general

Subject to paragraph (2) and sections 2007 and 2009 of this title, this chapter shall not prohibit the use of polygraph tests on prospective employees by any private employer whose primary business purpose consists of providing armored car personnel, personnel engaged in the design, installation, and maintenance of security alarm systems, [*information security personnel*] or other uniformed or plainclothes security personnel and whose function includes protection of--

(A) facilities, materials, or operations having a significant impact on the health or safety of any State or political subdivision thereof, or the national security of the United States, as determined under rules and regulations issued by the Secretary within 90 days after June 27, 1988, including--

(i) facilities engaged in the production, transmission, or distribution of electric or nuclear power,

(ii) public water supply facilities,

(iii) shipments or storage of radioactive or other toxic waste materials, and

(iv) public transportation.

(B) currency, negotiable securities, precious commodities or instruments, or proprietary information.

(2) Access

The exemption provided under this subsection shall not apply if the test is administered to a prospective employee who would not be employed to protect facilities, materials, operations, or assets referred to in paragraph (1).

* * * * *

Section 2006(f) exempts authorized manufacturers, distributors or dispensers of controlled substances.

Section 2007. Restrictions on use of exemptions

Section 2007 sets forth permissible uses of test results when performed by employers under conditions permitted by section 2006. Subsection (a) provides that adverse test results cannot provide the sole basis for discharge, discipline, or other discriminatory employment action. Subsection (b) sets forth the rights of the examinee, including the ability to terminate the test at any time; the right not to be asked degrading or needlessly intrusive questions; and the right not to be asked about religious, racial, or political beliefs or practices, sexual behavior, or union affiliations. This section also sets forth the procedures to be followed. The employer must, for example, provide the employee with notice of the time and place of the test, the right to obtain legal counsel, and what type of monitoring is to occur. The employee must read and sign a written notice of these provisions, and must be provided with an opportunity to review all questions in advance. The section sets forth additional requirements regulating the content and duration of the tests themselves. Subsection (c) requires the examiner to have a current State license in states requiring same, and to maintain a minimum of a $50,000 bond or professional liability insurance. All conclusions from the tests must be rendered in writing.

Section 2008. Disclosure of information

Section 2008 allows information obtained during the test to be revealed only by the examinee, or the examiner to the examinee, the employer, or to any court with proper process. The employer is generally prohibited from disclosing results, unless the disclosed information is an admission of criminal conduct.

Section 2009. Effect on other laws and agreements

Section 2009 makes clear that this law is not intended to preempt any state law or collective bargaining agreement that is more restrictive with respect to lie detector testing.